Pacific Alliance Medical Center
531 West College Street
Los Angeles, CA 90012

August 10, 2017

##C9770-L01-0123456 0001 00000001 **********9-OELZZ 123
SAMPLE A SAMPLE - EMPLOYEE
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

NOTICE OF DATA BREACH

Dear Sample A Sample:

At Pacific Alliance Medical Center (PAMC), we understand that the confidentiality and security of your personal information is critically important, and we are committed to protecting it. This letter is to notify you of a recent cyber incident that affected PAMC and may have resulted in a compromise of certain electronic files containing your personal information.

What Happened

On June 14, 2017, PAMC became aware that certain of its networked computer systems were being affected by a cyber incident. We suspect that the incident began on or shortly before that date. Shortly after becoming aware of the issue, PAMC's Information Technology Department completed a preliminary assessment and determined that certain networked computer systems had been infected by a computer virus that was encrypting (making unreadable) certain files on PAMC's computer network. PAMC promptly shut down our networked computer systems, initiated our incident response and recovery procedures, notified the Federal Bureau of Investigation, and began a privileged and confidential forensic investigation. Since then, we have decrypted (made readable again) the affected files and have taken, and are continuing to take, actions to restore the affected systems and prevent similar incidents.

Based on our investigation to date, we have no evidence that any unauthorized person actually viewed, retrieved, copied, or deleted any of your personal information. Typically, this type of computer virus, known as ransomware, is used to deny access to data and disrupt operations in order to extract money from the data owners—and not to steal data. However, this may not always be the case, and, thus, we are providing this notice as a precaution to patients or other individuals whose personal information may have been on servers affected by the virus.

0123456

What Information Was Involved

The personal information on the servers affected by the virus may have included: name, demographic information, date of birth, Social Security number, and employment information. We do not believe that the affected servers contained any credit or debit card or financial account information.

C9770-L01

What We Are Doing

We promptly notified the Federal Bureau of Investigation of the incident and continue our privileged and confidential forensic investigation. In addition, we have strengthened our virus detection and other systems and safeguards to prevent unauthorized persons from gaining access to our systems. We have also taken other steps to try to prevent similar incidents in the future. We note that this notification was not delayed as a result of any law enforcement investigation.

We notified the California Department of Public Health and are notifying the California Attorney General and the U.S. Department of Health and Human Services Office for Civil Rights of this incident.

As an extra precautionary measure to safeguard your information from potential misuse, we are partnering with Experian to provide its Experian IdentityWorks product for two years at no charge to you. A description of this product is provided in the attached material, which also contains instructions about how to enroll (including your personal activation code). If you choose to take advantage of the Experian IdentityWorks product, it will provide you with identity theft detection and resolution of identity theft services as described in the attached material. In order for us to activate this service, you must complete the enrollment process by November 30, 2017.

What You Can Do

It is important to reiterate that there is no evidence that an unauthorized person actually viewed, retrieved, copied, or removed your personal information. However, we also want to make you aware of certain precautionary measures that you might consider. We ask that you review the "Information About Identity Theft Protection" sheet enclosed with this letter. You should always remain vigilant by regularly reviewing your account statements and monitoring free credit reports, and immediately report to your financial institutions any suspicious activity involving one of your accounts. Please also consider enrolling in the Experian IdentityWorks product that we have offered to you.

For More Information

For more information, please call (877) 890-9332 anytime from 6am to 6pm PST, Monday through Friday, and 8am to 5pm PST, Saturday and Sunday, excluding major holidays.

We apologize for any inconvenience or concern that this incident may have caused you. We take the confidentiality and security of your personal information very seriously and will continue to take steps to help prevent a similar incident in the future.

Sincerely,

Brian Buchanan, CHC
Chief Compliance Officer
Pacific Alliance Medical Center
531 West College Street
Los Angeles, California 90012

Information About Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can also obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies using the phone numbers listed above. In order to request a security freeze, you will need to provide the following information:

0123456

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

C9770-L01

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Experian Identity Restoration: If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for two years from the date of this letter and does not require any action on your part at this time.

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks ^{SM} as a complimentary two-year membership. This product provides you with superior identity theft detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: November 30, 2017 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit2
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by November 30, 2017. Be prepared to provide engagement number DB02729 as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR TWO-YEAR EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE^{TM}:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Pacific Alliance Medical Center
531 West College Street
Los Angeles, CA 90012

August 10, 2017

##C9770-L02-0123456 0001 00000001 **********9-OELZZ 123
SAMPLE A SAMPLE - ADULT
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

NOTICE OF DATA BREACH

Dear Sample A Sample:

At Pacific Alliance Medical Center (PAMC), we understand that the confidentiality and security of your medical and personal information is critically important, and we are committed to protecting it. This letter is to notify you of a recent cyber incident that affected PAMC and may have resulted in a compromise of certain electronic files containing your medical or personal information.

What Happened

On June 14, 2017, PAMC became aware that certain of its networked computer systems were being affected by a cyber incident. We suspect that the incident began on or shortly before that date. Shortly after becoming aware of the issue, PAMC's Information Technology Department completed a preliminary assessment and determined that certain networked computer systems had been infected by a computer virus that was encrypting (making unreadable) certain files on PAMC's computer network. PAMC promptly shut down our networked computer systems, initiated our incident response and recovery procedures, notified the Federal Bureau of Investigation, and began a privileged and confidential forensic investigation. Since then, we have decrypted (made readable again) the affected files and have taken, and are continuing to take, actions to restore the affected systems and prevent similar incidents.

Based on our investigation to date, we have no evidence that any unauthorized person actually viewed, retrieved, copied, or deleted any of your medical or personal information. Typically, this type of computer virus, known as ransomware, is used to deny access to data and disrupt operations in order to extract money from the data owners—and not to steal data. However, this may not always be the case, and, thus, we are providing this notice as a precaution to patients or other individuals whose medical or personal information may have been on servers affected by the virus.

0123456

What Information Was Involved

The medical or personal information on the servers affected by the virus may have included: name, demographic information, date of birth, Social Security number, driver's license or identification card number, employment information, health insurance information, and health information, including, for example, treatment, diagnosis, and related information and medical images. We do not believe that the affected servers contained any credit or debit card or financial account information.

C9770-L02

What We Are Doing

We promptly notified the Federal Bureau of Investigation of the incident and continue our privileged and confidential forensic investigation. In addition, we have strengthened our virus detection and other systems and safeguards to prevent unauthorized persons from gaining access to our systems. We have also taken other steps to try to prevent similar incidents in the future. We note that this notification was not delayed as a result of any law enforcement investigation.

We notified the California Department of Public Health and are notifying the California Attorney General and the U.S. Department of Health and Human Services Office for Civil Rights of this incident.

As an extra precautionary measure to safeguard your information from potential misuse, we are partnering with Experian to provide its Experian IdentityWorks product for two years at no charge to you. A description of this product is provided in the attached material, which also contains instructions about how to enroll (including your personal activation code). If you choose to take advantage of the Experian IdentityWorks product, it will provide you with identity theft detection and resolution of identity theft services as described in the attached material. In order for us to activate this service, you must complete the enrollment process by November 30, 2017.

What You Can Do

It is important to reiterate that there is no evidence that an unauthorized person actually viewed, retrieved, copied, or removed your medical or personal information. However, we also want to make you aware of certain precautionary measures that you might consider. We ask that you review the "Information About Identity Theft Protection" sheet enclosed with this letter. You should always remain vigilant by regularly reviewing your account statements and monitoring free credit reports, and immediately report to your financial institutions any suspicious activity involving one of your accounts. Please also consider enrolling in the Experian IdentityWorks product that we have offered to you.

For More Information

For more information, please call (877) 890-9332 anytime from 6am to 6pm PST, Monday through Friday, and 8am to 5pm PST, Saturday and Sunday, excluding major holidays.

We apologize for any inconvenience or concern that this incident may have caused you. We take the confidentiality and security of your medical and personal information very seriously and will continue to take steps to help prevent a similar incident in the future.

Sincerely,

Brian Buchanan, CHC
Chief Compliance Officer
Pacific Alliance Medical Center
531 West College Street
Los Angeles, California 90012

Information About Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can also obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies using the phone numbers listed above. In order to request a security freeze, you will need to provide the following information:

0123456

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

C9770-L02

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Experian Identity Restoration: If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for two years from the date of this letter and does not require any action on your part at this time.

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks ^{SM} as a complimentary two-year membership. This product provides you with superior identity theft detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: November 30, 2017 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit2
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by November 30, 2017. Be prepared to provide engagement number DB02729 as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR TWO-YEAR EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE^{TM}:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Pacific Alliance Medical Center
531 West College Street
Los Angeles, CA 90012

August 10, 2017

##C9770-L03-0123456 0001 00000001 **********9-OELZZ 123
SAMPLE A SAMPLE JR. - DECEASED
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

NOTICE OF DATA BREACH

Dear Sample A Sample Jr.:

At Pacific Alliance Medical Center (PAMC), we understand that the confidentiality and security of medical and personal information is critically important, and we are committed to protecting it. This letter is to notify you, as next of kin to our former patient Sample A. Sample , of a recent cyber incident that affected PAMC and may have resulted in a compromise of certain electronic files containing your kin's medical or personal information.

What Happened

On June 14, 2017, PAMC became aware that certain of its networked computer systems were being affected by a cyber incident. We suspect that the incident began on or shortly before that date. Shortly after becoming aware of the issue, PAMC's Information Technology Department completed a preliminary assessment and determined that certain networked computer systems had been infected by a computer virus that was encrypting (making unreadable) certain files on PAMC's computer network. PAMC promptly shut down our networked computer systems, initiated our incident response and recovery procedures, notified the Federal Bureau of Investigation, and began a privileged and confidential forensic investigation. Since then, we have decrypted (made readable again) the affected files and have taken, and are continuing to take, actions to restore the affected systems and prevent similar incidents.

Based on our investigation to date, we have no evidence that any unauthorized person actually viewed, retrieved, copied, or deleted any of your kin's medical or personal information. Typically, this type of computer virus, known as ransomware, is used to deny access to data and disrupt operations in order to extract money from the data owners—and not to steal data. However, this may not always be the case, and, thus, we are providing this notice as a precaution to patients or other individuals whose medical or personal information may have been on servers affected by the virus.

0123456

What Information Was Involved

The medical or personal information on the servers affected by the virus may have included: name, demographic information, date of birth, Social Security number, driver's license or identification card number, employment information, health insurance information, and health information, including, for example, treatment, diagnosis, and related information and medical images. We do not believe that the affected servers contained any credit or debit card or financial account information.

C9770-L03

What We Are Doing

We promptly notified the Federal Bureau of Investigation of the incident and continue our privileged and confidential forensic investigation. In addition, we have strengthened our virus detection and other systems and safeguards to prevent unauthorized persons from gaining access to our systems. We have also taken other steps to try to prevent similar incidents in the future. We note that this notification was not delayed as a result of any law enforcement investigation.

We notified the California Department of Public Health and are notifying the California Attorney General and the U.S. Department of Health and Human Services Office for Civil Rights of this incident.

What You Can Do

It is important to reiterate that there is no evidence that an unauthorized person actually viewed, retrieved, copied, or removed your kin's medical or personal information. However, we also want to make you aware of certain precautionary measures that you might consider. We ask that you review the "Protecting Deceased Individuals" sheet enclosed with this letter. You should always remain vigilant by regularly reviewing account statements and monitoring free credit reports, and immediately report to the applicable financial institutions any suspicious activity.

For More Information

For more information, please call (877) 890-9332 anytime from 6am to 6pm PST, Monday through Friday, and 8am to 5pm PST, Saturday and Sunday, excluding major holidays.

We apologize for any inconvenience or concern that this incident may have caused you. We take the confidentiality and security of medical and personal information very seriously and will continue to take steps to help prevent a similar incident in the future.

Sincerely,

Brian Buchanan, CHC
Chief Compliance Officer
Pacific Alliance Medical Center
531 West College Street
Los Angeles, California 90012

Protecting Deceased Individuals

Experian has collaborated with the Identity Theft Resource Center (ITRC) to provide information on steps you can take when a deceased or incapacitated loved one is affected by a data compromise incident.

Decrease the risk of their identity theft regardless of age by following these steps:

1) Obtain at least 12 copies of the official death certificate when it becomes available. In some cases you will be able to use a photocopy, but some businesses will request an original death certificate. Since many death records are public, a business may require more than just a death certificate as proof.
2) If there is a surviving spouse or other joint account holders, make sure to immediately notify relevant credit card companies, banks, stock brokers, loan/lien holders, and mortgage companies of the death. They may require a copy of the death certificate to do this, as well as permission from the survivor, or other authorized account holders.
3) The executor or surviving spouse will need to discuss all outstanding debts and how they will be dealt with. You will need to transfer the account to another person or close the account. If you close the account, ask them to list it as: "Closed. Account holder is deceased."
4) Contact all credit reporting agencies (CRAs) (**see contact information below**), credit issuers, collection agencies, and any other financial institution that need to know of the death using the required procedures for each one. The following are general tips:

    a. Include the following information in all letters:
        i. Name and SSN of deceased
        ii. Last known address
        iii. Last 5 years of addresses
        iv. Date of birth
        v. Date of death
        vi. To speed up processing, include all requested documentation specific to that agency in the first letter
    b. Send the appropriate Court signed Executive papers
    c. Send all mail certified, return receipt requested.
    g. Keep copies of all correspondence, noting date sent and any response(s) you receive.
    h. Request a copy of the decedent's credit report. A review of each report will let you know of any active credit accounts that still need to be closed, or any pending collection notices. Be sure to ask for all contact information on accounts currently open in the name of the deceased (credit granters, collection agencies, etc.) so that you can follow through with those entities.
    i. Request that the report is flagged with the following alert: "Deceased. **Do not** issue credit. If an application is made for credit, notify the following person(s) immediately: (list the next surviving relative, executor/trustee of the estate and/or local law enforcement agency- noting the relationship)."

Note: Friends, neighbors or distant relatives do not have the same rights as a spouse or executor of the estate. They are classified as a third party and a CRA may not mail out a credit report or change data on a consumer file upon their request. If you fall into this classification and are dealing with a very unique situation, you may write to the CRA and explain the situation. They are handled on a case-by-case basis. You may also apply to the courts to be named as an executor of the estate.

Other groups to notify:

- Social Security Administration
- Insurance companies – auto, health, life, etc.
- Veteran's Administration - if the person was a former member of the military
- Immigration Services - if the decedent is not a U.S. citizen
- Department of Motor Vehicles if the person had a driver's license or state ID card. Also make sure that any vehicle registration papers are transferred to the new owners
- Agencies that may be involved due to professional licenses – bar association, medical licenses, cosmetician, etc.
- Any membership programs- video rental, public library, fitness club, etc.

0123456

Legal Notice: The information you obtain herein is not, nor intended to be, legal advice. We try to provide quality information but make no claims, promises or guarantees about the accuracy, completeness or adequacy of the information contained. As legal advice must be tailored to the specific circumstances of each case and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent legal counsel.

Specific Credit Reporting Agencies (CRAs) information for ordering a credit report or place a deceased flag:

Experian P.O. Box 9701 Allen, TX 75013 1-888-397-3742	
To order a credit report: A spouse can obtain a credit report by simply making the request through the regular channels - mail, phone and Internet. The spouse is legally entitled to the report. The executor of the estate can obtain a credit report but must write Experian with a specific request, a copy of the executor paperwork and the death certificate.	For requests or changes: A spouse or executor may change the file to show the person as deceased via written request. A copy of the death certificate and in the case of the executor, the executor's paperwork must be included with the request. After any changes, Experian will send an updated credit report to the spouse or executor for confirmation that a deceased statement has been added to the credit report. This is important as executors and spouse can request other types of "changes" that we may not be able to honor. If identity theft is a stated concern, Experian will add a security alert after the file has been changed to reflect the person as deceased. If there are additional concerns, Experian will add a general statement to the file at the direction of the spouse/executor. The spouse/executor must state specifically what they want the general statement to say, such as "Do not issue credit."
Equifax Information Services LLC Office of Consumer Affairs P.O. Box 105139, Atlanta, GA 30348 1-800-685-1111	
To order a credit report: Equifax requests that the spouse, attorney or executor of the estate submit a written request to receive a copy of the deceased consumer's' file. The request should include the following: A copy of a notarized document stating that the requestor is authorized to handle the deceased consumer's affairs (i.e.: Order from a Probate Court or Letter of Testamentary)	For requests or changes: Equifax requests that a spouse, attorney or executor of the estate submit a written request if they would like to place a deceased indicator on the deceased consumer's file. The written request should include a copy of the consumer's death certificate. The request should be sent to the address listed above. Upon receipt of the death certificate, Equifax will attempt to locate a file for the deceased consumer and place a death notice on the consumer's file. In addition, Equifax will place a seven year promotional block on the deceased consumer's file. Once Equifax's research is complete, they will send a response back to the spouse, attorney, or executor of the estate.
TransUnion P.O. Box 6790 Fullerton, CA 92834 1-800-888-4213	
To order a credit report: TransUnion requires proof of a power of attorney, executor of estate, conservatorship or other legal document giving the requestor the legal right to obtain a copy of the decedent's credit file. If the requestor was married to the deceased and the address for which the credit file is being mailed to is contained on the decedent's credit file, then TransUnion will mail a credit file to the surviving spouse. If the deceased is a minor child of the requestor, TransUnion will mail a credit file to the parent upon receipt of a copy of the birth certificate or death certificate naming the parent as requestor.	For requests or changes: Placing a "decease alert" on reports: TransUnion will accept a request to place a temporary alert on the credit file of a deceased individual from any consumer who makes such a request and identifies themselves as having a right to do so. The requestor's phone number is added to the temporary, three month alert. Upon receipt of a verifiable death certificate, TransUnion will entirely suppress the decedent's credit file and so note it as a deceased consumer. TransUnion will not mail out a copy of its contents without the requirements mentioned above. If you suspect fraud, TransUnion suggests a call to their fraud unit at 800-680-7289. It will place the temporary alert over the phone and advise the requestor of what needs to be sent to suppress the credit file and to disclose a copy of its contents. Requests can also be emailed to fvad@transunion.com.

Pacific Alliance Medical Center
531 West College Street
Los Angeles, CA 90012

August 10, 2017

##C9770-L04-0123456 0001 00000001 **********9-OELZZ 123
TO THE PARENT OR LEGAL GUARIDAN OF:
SAMPLE A SAMPLE - MINOR
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

NOTICE OF DATA BREACH

Dear Parent or Legal Guardian of Sample A Sample:

At Pacific Alliance Medical Center (PAMC), we understand that the confidentiality and security of medical and personal information is critically important, and we are committed to protecting it. This letter is to notify you of a recent cyber incident that affected PAMC and may have resulted in a compromise of certain electronic files containing your minor's medical or personal information.

What Happened

On June 14, 2017, PAMC became aware that certain of its networked computer systems were being affected by a cyber incident. We suspect that the incident began on or shortly before that date. Shortly after becoming aware of the issue, PAMC's Information Technology Department completed a preliminary assessment and determined that certain networked computer systems had been infected by a computer virus that was encrypting (making unreadable) certain files on PAMC's computer network. PAMC promptly shut down our networked computer systems, initiated our incident response and recovery procedures, notified the Federal Bureau of Investigation, and began a privileged and confidential forensic investigation. Since then, we have decrypted (made readable again) the affected files and have taken, and are continuing to take, actions to restore the affected systems and prevent similar incidents.

Based on our investigation to date, we have no evidence that any unauthorized person actually viewed, retrieved, copied, or deleted any of your minor's medical or personal information. Typically, this type of computer virus, known as ransomware, is used to deny access to data and disrupt operations in order to extract money from the data owners—and not to steal data. However, this may not always be the case, and, thus, we are providing this notice as a precaution to patients or other individuals whose medical or personal information may have been on servers affected by the virus.

0123456

What Information Was Involved

The medical or personal information on the servers affected by the virus may have included: name, demographic information, date of birth, Social Security number, driver's license or identification card number, employment information, health insurance information, and health information, including, for example, treatment, diagnosis, and related information and medical images. We do not believe that the affected servers contained any credit or debit card or financial account information.

C9770-L04

What We Are Doing

We promptly notified the Federal Bureau of Investigation of the incident and continue our privileged and confidential forensic investigation. In addition, we have strengthened our virus detection and other systems and safeguards to prevent unauthorized persons from gaining access to our systems. We have also taken other steps to try to prevent similar incidents in the future. We note that this notification was not delayed as a result of any law enforcement investigation.

We notified the California Department of Public Health and are notifying the California Attorney General and the U.S. Department of Health and Human Services Office for Civil Rights of this incident.

As an extra precautionary measure to safeguard your minor's information from potential misuse, we are partnering with Experian to provide its Experian IdentityWorks product for two years at no charge to you. A description of this product is provided in the attached material, which also contains instructions about how to enroll (including your personal activation code). If you choose to take advantage of the Experian IdentityWorks product, it will provide your minor with identity theft detection and resolution of identity theft services as described in the attached material. In order for us to activate this service, you must complete the enrollment process by November 30, 2017.

What You Can Do

It is important to reiterate that there is no evidence that an unauthorized person actually viewed, retrieved, copied, or removed your minor's medical or personal information. However, we also want to make you aware of certain precautionary measures that you might consider. We ask that you review the "Information About Identity Theft Protection" sheet enclosed with this letter. You should always remain vigilant by regularly reviewing account statements and monitoring free credit reports, and immediately report to the applicable financial institutions any suspicious activity. Please also consider enrolling in the Experian IdentityWorks product that we have offered to you.

For More Information

For more information, please call (866) 579-5479 anytime from 6am to 6pm PST, Monday through Friday, and 8am to 5pm PST, Saturday and Sunday, excluding major holidays.

We apologize for any inconvenience or concern that this incident may have caused you. We take the confidentiality and security of medical and personal information very seriously and will continue to take steps to help prevent a similar incident in the future.

Sincerely,

Brian Buchanan, CHC
Chief Compliance Officer
Pacific Alliance Medical Center
531 West College Street
Los Angeles, California 90012

Information About Identity Theft Protection

We recommend that you regularly review statements from your minor's accounts and periodically obtain your minor's credit report from one or more of the national credit reporting companies. You may obtain a free copy of your minor's credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your minor's credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your minor's credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your minor's account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are also two types of fraud alerts that you can place on your minor's credit report to put your minor's creditors on notice that your minor may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your minor's credit report if you suspect your minor has been, or is about to be, a victim of identity theft. An initial fraud alert stays on your minor's credit report for at least 90 days. You may have an extended alert placed on your minor's credit report if your minor has already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your minor's credit report for seven years. You can place a fraud alert on your minor's credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your minor's credit file, so that no new credit can be opened in your minor's name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your minor's credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your minor's ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your minor's credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can also obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies using the phone numbers listed above. In order to request a security freeze, you will need to provide the following information:

0123456

1. Your minor's full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If your minor have moved in the past five (5) years, provide the addresses where your minor has lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If your minor is a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If your minor is not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

C9770-L04

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your minor's credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your minor's credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your minor's credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Experian Identity Restoration: If you believe there was fraudulent use of your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your minor's credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your minor's identity to its proper condition).

Please note that this offer is available to your minor for two years from the date of this letter and does not require any action on your part at this time.

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks ^{SM} as a complimentary two-year membership. This product provides your minor with superior identity theft detection and resolution of identity theft. To start monitoring your minor's personal information please follow the steps below:

- Ensure that you **enroll by**: November 30, 2017 (Your minor's code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/minorplus2
- Provide your minor's **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 866-579-5479 by November 30, 2017. Be prepared to provide engagement number DB02878 as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR MINOR'S TWO-YEAR EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll your minor in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your minor's credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE^{TM}:** Your minor receives the same high-level of Identity Restoration support even after your minor's Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What you can do to protect your minor's information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your minor's account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.